

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM  
Internationales Büro



INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE  
INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation <sup>7</sup> : H04L 9/06, G06F 1/00	A1	(11) Internationale Veröffentlichungsnummer: WO 00/19657 (43) Internationales Veröffentlichungsdatum: 6. April 2000 (06.04.00)
---	----	--

(21) Internationales Aktenzeichen: PCT/EP99/07019  
(22) Internationales Anmeldedatum: 20. September 1999  
(20.09.99)

(30) Prioritätsdaten:  
198 45 096.6 30. September 1998 (30.09.98) DE  
199 36 890.2 5. August 1999 (05.08.99) DE

(71) Anmelder (für alle Bestimmungsstaaten ausser US): KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(71) Anmelder (nur für DE): PHILIPS CORPORATE INTELLECTUAL PROPERTY GMBH [DE/DE]; Habsburgerallee 11, D-52066 Aachen (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder (nur für US): PHILIPP, Stefan [DE/NL]; Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

(74) Anwalt: PETERS, Carl, H.; Internationaal Octroobureau B.V., Prof. Holstlaan 6, NL-5656 AA Eindhoven (NL).

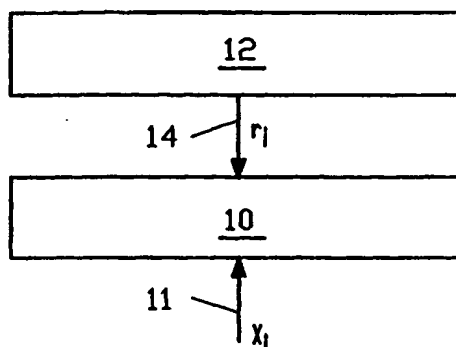
(81) Bestimmungsstaaten: JP, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht

Mit internationalem Recherchenbericht.  
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: ENCODING METHOD FOR CARRYING OUT CRYPTOGRAPHIC OPERATIONS

(54) Bezeichnung: VERSCHLÜSSELUNGSVERFAHREN ZUM AUSFÜHREN VON KRYPTOGRAPHISCHEN OPERATIONEN



(57) Abstract

The invention relates to an encoding method according to which a partial cryptographic operation is carried out by data which are digitally stored as at least one data bit word in a memory cell (1) or a register. To provide such a system which effectively prevents successful cryptanalysis by observation of a current consumption of a data processing unit, the invention provides for a data bit word generated on the basis of random numbers to be stored in a memory cell (10) before a data bit word is written into same.

(57) Zusammenfassung

Um ein Verschlüsselungsverfahren, bei dem eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle (10) bzw. einem Register gespeicherten Daten ausgeführt wird, zur Verfügung zu stellen, welches eine erfolgreiche Kryptoanalyse mittels Beobachtung eines Stromverbrauches eines Datenverarbeitungsgerätes wirksam verhindert, wird vorgeschlagen, dass vor dem Schreiben eines Datenbitwortes in eine Speicherzelle (10) in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.

# **LEDIGLICH ZUR INFORMATION**

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Verschlüsselungsverfahren zum Ausführen von kryptographischen Operationen.

### Technisches Gebiet

Die Erfindung betrifft ein Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle bzw. einem Register gespeicherten Daten ausgeführt wird, gemäß dem

5 Oberbegriff des Anspruchs 1.

### Stand der Technik

In vielen Datenverarbeitungsgeräten dienen kryptographische Operationen zum Schutz des Betriebes dieser Geräte bzw. zum Schutz von in dem Gerät transportierte Daten.

10 Die hierfür notwendigen Berechnungsoperationen werden dabei sowohl von Standard-Rechenwerken als auch von dedizierten Crypto-Rechenwerken durchgeführt. Ein typisches Beispiel für letzteres sind Chipkarten bzw. IC-Karten. Bei derartigen kryptographischen Berechnungen ist es oftmals notwendig, entsprechende Speicherbereiche bzw. Register des Datenverarbeitungsgerätes mit Operanden zu initialisieren. Bei den in diesem Zusammenhang

15 verwendeten Daten bzw. Zwischenergebnissen handelt es sich üblicherweise um sicherheitsrelevante Informationen, wie beispielsweise kryptographische Schlüssel oder Operanden.

Zur Berechnung der kryptographischen Algorithmen werden in den Datenverarbeitungsgeräten logische Verknüpfungen zwischen Operanden bzw.

20 Zwischenergebnissen durchgeführt. In Abhängigkeit von der verwendeten Technologie führen diese Operationen, insbesondere das Laden von leeren oder zuvor gelöschten Speicherbereichen bzw. Register mit Daten, zu einem erhöhten Stromverbrauch der Datenverarbeitungsgeräte. Bei komplementärer Logik, wie beispielsweise der CMOS-Technik, tritt ein erhöhter Stromverbrauch dann auf, wenn der Wert einer Bit-Speicherzelle

25 geändert wird, d.h. sein Wert sich von "0" auf "1" bzw. von "1" auf "0" ändert. Der erhöhte Verbrauch hängt dabei von der Anzahl der im Speicher bzw. Register geänderten Bitstellen ab. Mit anderen Worten lässt das Laden eines zuvor gelöschten Registers einen Stromverbrauch proportional zum Hamminggewicht des in das leere Register geschriebenen Operanden (=Anzahl der Bits mit dem Wert "1") ansteigen. Durch eine entsprechende Analyse dieser

Stromänderung könnte es möglich sein, Informationen über die berechneten Operationen zu extrahieren, so dass eine erfolgreiche Kryptoanalyse von geheimen Operanden, wie beispielsweise kryptographischen Schlüsseln, möglich ist. Mittels Durchführung mehrerer Strommessungen am Datenverarbeitungsgerät könnten beispielsweise bei sehr kleinen  
5 Signaländerungen eine hinreichende Extraktion der Informationen ermöglicht werden. Andererseits könnten mehrere Strommessungen eine ggf. erforderliche Differenzbildung ermöglichen. Diese Art der Kryptoanalyse wird auch als "Differential Power Analysis" bezeichnet, mittels derer ein Außenstehender durch reine Beobachtung von Änderungen des Stromverbrauches des Datenverarbeitungsgerätes eine ggf. unberechtigte Kryptoanalyse der  
10 kryptographischen Operationen, Algorithmen, Operanden bzw. Daten erfolgreich ausführen kann.

Bei einer aus der EP 0 482 975 B1 bekannten Speicherkarte mit Mikroschaltung  
15 und wenigstens einem Speicher, die an einem Datenverarbeitungsorgan angeschlossen ist, wobei das Datenverarbeitungsorgan von einem Datensignal von außerhalb der Karte gesteuert wird und als Antwort auf dieses Datensignal zu einem Zeitpunkt ein Befehlssendesignal abgibt, welches um eine vorbestimmte Dauer (T) bzgl. des Empfangs des Datensignals verzögert ist, wird zum Erhöhen des Schutzes die Zeitdauer (T) auf Zufallsbasis zeitlich variabel gewählt.  
20 Eine Kryptoanalyse auf der Basis einer Stromänderung beim Beschreiben des Speichers kann dieses System jedoch nicht verhindern.

#### Darstellung der Erfindung, Aufgabe, Lösung, Vorteile

Es ist Aufgabe der vorliegenden Erfindung, ein verbessertes Verfahren der  
25 obengenannten Art zur Verfügung zu stellen, welches die obengenannten Nachteile beseitigen und eine erfolgreiche Kryptoanalyse mittels Beobachtung eines Stromverbrauches eines Datenverarbeitungsgerätes wirksam verhindert.

Diese Aufgabe wird durch ein Verfahren der o.g. Art mit den in Anspruch 1 gekennzeichneten Merkmalen gelöst.

30 Dazu ist es erfindungsgemäß vorgesehen, dass vor dem Schreiben eines Datenbitwortes in eine Speicherzelle in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.

Dies hat den Vorteil, dass eine nicht vorbestimmte oder vorbestimmbare Vorinitialisierung vorliegt, welche aus Änderungen des Stromverbrauches beim Schreiben in

die Speicherzelle keinen Rückschluß auf das in die Speicherzelle geschriebene Datenbitwort zulässt. Beim Einschreiben von Daten in derartig vorinitialisierte Speicherzellen ändert sich der Stromverbrauch lediglich abhängig von einer Differenz des Hamminggewichtes der eingeschriebenen Daten von der unbekannten Zufallszahl, so daß auch diese Differenz und damit die Änderung des Stromverbrauches zufällig und nicht vorherbestimmbar ist.

Bei der Umsetzung des Verfahrens bestehen verschiedene Möglichkeiten. Nach einer bevorzugten Vorgehensweise wird das auf Zufallszahlen basierende Bitwort von einem Rechenwerk in die Speicherzelle geschrieben. Alternativ wird das auf Zufallszahlen basierende Bitwort über eine direkte Verbindung zwischen einer Zufallszahlenquelle und der Speicherzelle in letztere geschrieben.

Eine zeitliche Korrelation zwischen dem Einschreiben der Zufallszahl in eine Speicherzelle und der kryptographische Teiloperation wird dadurch vermieden, dass das auf Zufallszahlen basierende Bitwort zeitlich beabstandet vor der kryptographische Teiloperation in der Speicherzelle gespeichert wird.

15

#### Kurze Beschreibung der Zeichnungen

Nachstehend wird die Erfindung anhand der beigelegten Zeichnungen näher erläutert. Diese zeigt in der einzigen Fig. ein Ablaufschema einer bevorzugten Ausführungsform eines erfindungsgemäßen Verfahrens.

20

#### Bester Weg zur Ausführung der Erfindung

Wie in der einzigen Fig. veranschaulicht, ist eine Speicherzelle 10 bzw. ein Register zum Einschreiben bzw. Abspeichern von Daten  $x_i$  in Form eines Datenbitwortes über eine Verbindung 11 vorgesehen. Bevor jedoch der Operand  $x_i$  in die Speicherzelle 10 eingeschrieben wird, werden von einer Zufallszahlenquelle 12 Zufallszahlen erzeugt und über eine direkte Verbindung 14 in die Speicherzelle 10 eingeschrieben bzw. in dieser abgespeichert. Mit anderen Worten wird die Speicherzelle 10 mit einem Zufallswert  $r_i$  initialisiert. Alternativ zu der dargestellten Ausführungsform kann das Einschreiben des Zufallswertes  $r_i$  auch über die Verbindung 11 von einem Rechenwerk erfolgen, welches zuvor den Zufallswert von der Zufallszahlenquelle 12 erhalten hat.

30

Der Zeitpunkt dieser Vorinitialisierung ist beliebig wählbar und erfolgt bevorzugt nicht unmittelbar vor der kryptographischen Operation. Zweckmäßigerweise erfolgt eine wiederholte Vorinitialisierung der Speicherbereich bzw. Register mit sich ändernden Zufallszahlen.

- Werden die so vorinitialisierten Speicherbereiche bzw. Register im Zuge einer kryptographischen Operation mit Daten  $x_i$  geladen, ändert sich der Stromverbrauch nun lediglich abhängig von einer Differenz des Hamminggewichtes des Operanden  $x_i$  und des Hamminggewichtes der unbekannten Zufallszahl. Ausgehend von diesem zufälligen
- 5 Differenzwert ist es nun nicht möglich, Angaben über die verwendeten Operanden bzw. Zwischenergebnisse abzuleiten.

## BEZUGSZEICHENLISTE:

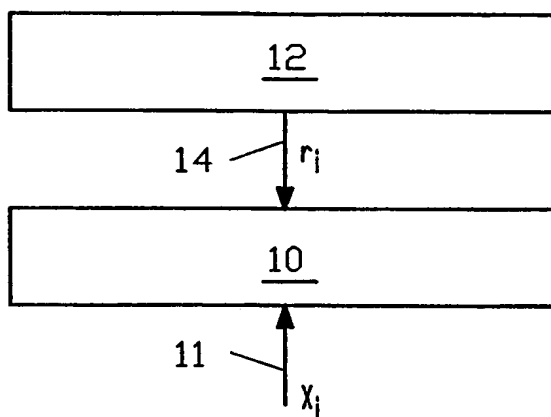
	10	Speicherzelle / Register
	11	Verbindung
	12	Zufallszahlenquelle
	Verbindung	
5	Xi	Daten
	Ti	Zufallswert

## PATENTANSPRÜCHE:

1. Verschlüsselungsverfahren, wobei wenigstens eine kryptographische Teiloperation von digital als wenigstens ein Datenbitwort in einer Speicherzelle (10) bzw. einem Register gespeicherten Daten ausgeführt wird,  
dadurch gekennzeichnet, dass  
5 vor dem Schreiben eines Datenbitwortes in eine Speicherzelle (10) in dieser ein Datenbitwort gespeichert wird, welches auf Zufallszahlen basierend erzeugt wird.
2. Verschlüsselungsverfahren nach Anspruch 1,  
dadurch gekennzeichnet, dass  
10 das auf Zufallszahlen basierende Bitwort von einem Rechenwerk in die Speicherzelle (10) geschrieben wird.
3. Verschlüsselungsverfahren nach Anspruch 1,  
dadurch gekennzeichnet, dass  
15 das auf Zufallszahlen basierende Bitwort über eine direkte Verbindung zwischen einer Zufallszahlenquelle (12) und der Speicherzelle (10) in letztere geschrieben wird.
4. Verschlüsselungsverfahren nach einem der vorhergehenden Ansprüche,  
20 dadurch gekennzeichnet, dass  
das auf Zufallszahlen basierende Bitwort zeitlich beabstandet vor der kryptographische Teiloperation in der Speicherzelle (10) gespeichert wird.



1/1



526 Rec'd DCT/PTO

26 MAY 2000

**THIS PAGE BLANK (USPTO)**

# INTERNATIONAL SEARCH REPORT

Int. Application No.

PCT/EP 99/07019

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/06 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 002 388 A (IBM) 13 June 1979 (1979-06-13) abstract page 34, last paragraph -page 35, paragraph 2 page 78, last paragraph -page 79, line 2	1
A	PATENT ABSTRACTS OF JAPAN vol. 014, no. 089 (E-0891), 19 February 1990 (1990-02-19) & JP 01 298829 A (NEC CORP), 1 December 1989 (1989-12-01) abstract	1-3

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

### \* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"Z" document member of the same patent family

Date of the actual completion of the international search

20 January 2000

Date of mailing of the international search report

28/01/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax (+31-70) 340-3016

Authorized officer

Holper, G

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. l. Application No

PCT/EP 99/07019

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0002388 A	13-06-1979	US 4386234 A	31-05-1983
		CA 1149483 A	05-07-1983
		JP 1355657 C	24-12-1986
		JP 54087033 A	11-07-1979
		JP 61022316 B	31-05-1986
JP 01298829 A	01-12-1989	NONE	

# INTERNATIONALER RECHERCHENBERICHT

Int. Sonstiges Abkürzungszeichen

PCT/EP 99/07019

## A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 H04L9/06 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der Internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 002 388 A (IBM) 13. Juni 1979 (1979-06-13) Zusammenfassung Seite 34, letzter Absatz -Seite 35, Absatz 2 Seite 78, letzter Absatz -Seite 79, Zeile 2	1
A	PATENT ABSTRACTS OF JAPAN vol. 014, no. 089 (E-0891), 19. Februar 1990 (1990-02-19) & JP 01 298829 A (NEC CORP), 1. Dezember 1989 (1989-12-01) Zusammenfassung	1-3

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfindeterischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindeterischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der Internationalen Recherche

20. Januar 2000

Abmeldedatum des internationalen Recherchenberichts

28/01/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentaan 2

NL - 2280 HV Rijswijk

Tel. (+31-70) 340-2040, Tx. 31 851 epo nl,

Fax: (+31-70) 340-3018

Bevollmächtigter Bediensteter

Holper, G

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Int. Internationales Aktenzeichen

PCT/EP 99/07019

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
EP 0002388 A	13-06-1979	US 4386234 A CA 1149483 A JP 1355657 C JP 54087033 A JP 61022316 B	31-05-1983 05-07-1983 24-12-1986 11-07-1979 31-05-1986
JP 01298829 A	01-12-1989	KEINE	

## PATENT COOPERATION TREATY

2132

PCT

NOTIFICATION CONCERNING  
DOCUMENT TRANSMITTED

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents  
United States Patent and Trademark  
Office  
Box PCT  
Washington, D.C. 20231  
ETATS-UNIS D'AMERIQUE

RECEIVED

NOV 24 2000

Technology Center 2100

in its capacity as designated Office

Date of mailing (day/month/year)

25 September 2000 (25.09.00)

International application No.

PCT/EP99/07019

International filing date (day/month/year)

20 September 1999 (20.09.99)

Applicant

KONINKLIJKE PHILIPS ELECTRONICS N.V. et al

The International Bureau transmits herewith the following documents and number thereof:

\_\_\_\_\_ cop(ies) of priority document(s) (Rule 17.2(a))

The International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

R. Chrem

Telephone No.: (41-22) 338.83.38

**THIS PAGE BLANK (USPTO)**



## PATENT COOPERATION TREATY

PCT

NOTIFICATION CONCERNING  
SUBMISSION OR TRANSMITTAL  
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

From the INTERNATIONAL BUREAU

To:

PETERS, Carl, H.  
Internationaal Octrooibureau B.V.  
Prof. Holstlaan 6  
NL-5656 AA Eindhoven  
PAYS-BAS

Date of mailing (day/month/year) 25 September 2000 (25.09.00)	<b>IMPORTANT NOTIFICATION</b>
Applicant's or agent's file reference PHD 99.100WO	
International application No. PCT/EP99/07019	International filing date (day/month/year) 20 September 1999 (20.09.99)
International publication date (day/month/year) 06 April 2000 (06.04.00)	Priority date (day/month/year) 30 September 1998 (30.09.98)
Applicant KONINKLIJKE PHILIPS ELECTRONICS N.V. et al	

1. The applicant is hereby notified of the date of receipt (except where the letters "NR" appear in the right-hand column) by the International Bureau of the priority document(s) relating to the earlier application(s) indicated below. Unless otherwise indicated by an asterisk appearing next to a date of receipt, or by the letters "NR", in the right-hand column, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).
2. This updates and replaces any previously issued notification concerning submission or transmittal of priority documents.
3. An asterisk(\*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b). In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.
4. The letters "NR" appearing in the right-hand column denote a priority document which was not received by the International Bureau or which the applicant did not request the receiving Office to prepare and transmit to the International Bureau, as provided by Rule 17.1(a) or (b), respectively. In such a case, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

<u>Priority date</u>	<u>Priority application No.</u>	<u>Country or regional Office or PCT receiving Office</u>	<u>Date of receipt of priority document</u>
30 Sept 1998 (30.09.98)	198 45 096.6	DE	19 Sept 2000 (19.09.00) *
05 Aug 1999 (05.08.99)	199 36 890.2	DE	23 Nove 1999 (23.11.99)

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland  Facsimile No. (41-22) 740.14.35	Authorized officer  R. Chrem  Telephone No. (41-22) 338.83.38
--	---

**THIS PAGE BLANK (USPTO)**

mH

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

### INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts <b>PHD 99.100WO</b>	<b>WEITERES VORGEHEN</b> siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
Internationales Aktenzeichen <b>PCT/EP 99/ 07019</b>	Internationales Anmeldedatum (Tag/Monat/Jahr) <b>20/09/1999</b>
	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) <b>30/09/1998</b>
Anmelder  <b>KONINKLIJKE PHILIPS ELECTRONICS N.V. et al.</b>	

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.



Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

#### 1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.



Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das



in der internationalen Anmeldung in Schriftlicher Form enthalten ist.



zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.



bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.



bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.



Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.



Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

#### 4. Hinsichtlich der Bezeichnung der Erfindung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut von der Behörde wie folgt festgesetzt:

#### 5. Hinsichtlich der Zusammenfassung



wird der vom Anmelder eingereichte Wortlaut genehmigt.



wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der Zeichnungen ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1



wie vom Anmelder vorgeschlagen



keine der Abb.



weil der Anmelder selbst keine Abbildung vorgeschlagen hat.



weil diese Abbildung die Erfindung besser kennzeichnet.

**THIS PAGE BLANK (USPTO)**

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES  
 IPK 7 H04L9/06 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	EP 0 002 388 A (IBM) 13. Juni 1979 (1979-06-13) Zusammenfassung Seite 34, letzter Absatz -Seite 35, Absatz 2 Seite 78, letzter Absatz -Seite 79, Zeile 2 ----	1
A	PATENT ABSTRACTS OF JAPAN vol. 014, no. 089 (E-0891), 19. Februar 1990 (1990-02-19) & JP 01 298829 A (NEC CORP), 1. Dezember 1989 (1989-12-01) Zusammenfassung -----	1-3

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

\* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderscher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

20. Januar 2000

Absendedatum des internationalen Recherchenberichts

28/01/2000

Name und Postanschrift der Internationalen Recherchenbehörde  
 Europäisches Patentamt, P.B. 5818 Patentlaan 2  
 NL - 2280 HV Rijswijk  
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Holper, G

**THIS PAGE BLANK (USPTO)**

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/07019

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0002388 A	13-06-1979	US 4386234 A	31-05-1983
		CA 1149483 A	05-07-1983
		JP 1355657 C	24-12-1986
		JP 54087033 A	11-07-1979
		JP 61022316 B	31-05-1986
<hr/>			
JP 01298829 A	01-12-1989	NONE	
<hr/>			

**THIS PAGE BLANK (USPTO)**